Ontrack®

Ensuring the secure sanitisation and destruction of end-of-life data

Table of contents

o Introduction .... Page 1

o Protecting data, the true challenge of our time .... Page 2

o What is the secure sanitisation of data? .... Page 3

o To adhere to legal requirements and industry standards, ... Page 4
the secure sanitisation of data is not a choice but a requirement

o Data recovery and data protection .... Page 5 - 6

o Technical measures for secure sanitisation .... Page 7 - 8

o Devices subject to sanitisation .... Page 9

o Professional tools to perform secure data sanitisation .... Page 10 - 12

o Conclusion .... Page 13

Introduction

Data security is a high priority, and it's even more relevant when referring to the safety of personal and corporate data. To prevent the possibility of unauthorised access to data, it is necessary to ensure that the information stored within legacy or redundant IT infrastructure has the appropriate and rigorous level of protection when its life cycles come to an end. Organisations are consisently investing in security, but these efforts are usually focused on the protection of IT systems while they are still in use and not during the disposition of assets. Organisations need to be more careful than ever when it comes to the sanitisation and destruction of end of life data. The introduction of data privacy acts such as the European General Data Protection Regulation (GDPR), Australia's Privacy Principles (APP), and Canada's Personal Information Protection and Electronic Data Act (PIPEDA) means that organisations need to have an increased focus on ensuring that data is sanitized in the correct manor.

The fundamental question that arises is how companies protect data when they decommission, dispose of, reuse, or recycle their computer systems. Fortunately, there is a solution. With a complete sanitisation strategy, organisations can protect their data by eliminating it permanently from computers and other electronic devices. Whether that's due to the expiry of device lease agreements, or the termination of the life cycle of hardware, ensuring correct sanitisation and destruction procedures are in place is vital to prevent data breaches.

In this ebook, readers will find an overview of the main operational and regulatory aspects concerning the sanitisation and destruction of data, and suggestions for a complete strategy including planning, specialised tools and verification.

Protecting data, the true challenge of our time

With increasing rates of cybercrime and large penalties for data breaches, the protection of sensitive data is a challenge for the majority of businesses. As previously mentioned, organisations must ensure they safeguard their computer systems at all times, even when they reach the end of their life cycle. It can be difficult to comprehend the scale of the average company's data footprint. Today, organisations must manage desktops and laptops, multi-disk servers, and tape backups as well as mobile devices, memory cards, virtual environments and cloud deployments. It's more important than ever that organisations manage every detail of their data securely – and in compliance with regulations - not just in storage and transit, but also at the end of its lifecycle.

When data erasure operations are not completed or properly carried out, sensitive and confidential files may be left behind on devices. Organisations are put at risk of a data breach or theft, when intellectual property, private documents, and email, as well as financial and health records, and other critical information are not securely wiped from storage media. Having the correct processes in place will not only protect organisations from potential data breaches but will also ensure they're adhering to international standards.

The introduction of GDPR in 2018 meant that those that had thought securely sanitising files could be achieved by clicking "Delete" and then "Empty Bin", had to change their approach radically. Even reformatting a disk is not enough to guarantee compliance with European GDPR: if a file is no longer visible on your PC, this does not necessarily mean that the data is no longer present on the device.
It's not just Europe that has seen new laws introduced to protect the privacy of data. The United States government added legislation and regulatory requirements surrounding the protection of data under the Obama Presidency. The Consumer Privacy Bill of Rights embraces a dynamic model of how to enable ongoing innovation in new information technologies while offering strong privacy protection – including a requirement for the deletion of data.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).*

What is the secure sanitisation of data?

Decommissioning, disposing or reusing your IT assets currently represents one of the most vulnerable moments for your data. Most companies don't take appropriate precautions for the retirement of each PC, mobile device, server or other electronic devices. In the case of retiring legacy IT infrastructure, all information (including personal data) will remain completely visible and accessible to anyone who has access to that hardware if it is not sanitised or destroyed correctly.

Many people believe that native deletion options, such as the use of the 'Delete' command on a selection of files, choosing to 'Empty Trash' or 'Format' the drive are all secure sanitisation solutions, capable of eliminating all traces of deleted files quickly and permanently. Unfortunately, the fact that the content is no longer visible does not necessarily mean that it is no longer present on the storage media system. Commands, such as those previously mentioned, delete the pointers to the operating system where your files are located.

Imagine you are browsing through a book. In the beginning, there is an index indicating the location of chapters through page numbers. If you get rid of this index, you would be mistaken in imagining that it equates to the deletion of the contents of the book. You won't know what position a particular chapter is, but the book content nevertheless remains there, and if you 'search' through it you won't have any trouble in finding what you are looking for. Data sanitisation is essential; it's different from the simple act of deleting file pointers and the contents of the files themselves. In fact, none of the original information on your device is recoverable once it's been securely sanitised. Returning to the example of the book, it is as if by removing the index, all the pages of the chapters in the book are also deleted.

Overwriting, of which we will talk more about in section 6, is a technical measure for the secure sanitisation of data. It eliminates not only the pointers to the files but also the files themselves. Securely sanitised data is no longer present on the media itself, and cannot be retrieved, not only with the use of specific software but also by data recovery specialists.

The secure sanitisation of data is not a choice but a necessity

The sanitisation of data, rather than being perceived as only required by law, should be adopted as best practice for the protection of data held by the company, regardless of the type of business. Protecting the personal information of customers, suppliers, and employees is ultimately a best practice rule; as is protecting confidential data related to the business such as intellectual property rights, development projects for new products, and accounting information, etc.

Many organisations have taken the protection of information and sensitive data; according to MarketsandMarkets, the global cybersecurity market is booming. Cybersecurity-related spending is on track to surpass $133 billion in 2022, and the market has grown more than 30x in 13 years. However, all investments and information stored within protected IT systems become insecure if you ignore adequate security as soon as the hardware is discarded; leaving the existing data vulnerable. Protecting personal data and digital information doesn't mean it has to be a burden on your existing IT procedures but rather an investment in security for the benefit of the company and to protect those who interact with it.

Many larger businesses follow IT frameworks such as TOGAF and ITIL security management process, which provide guidelines for IT architecture compliance as well as how to incorporate security in the management of the organisation. Having these in place helps corporations continue to develop their IT infrastructure within a secure framework. The importance of secure sanitisation has to be acknowledged throughout the company. As a policy, it should be circulated amongst the employees, so they have a clear understanding. As a logical consequence, the IT departments should be equipped with adequate tools in order to perform all-new procedures correctly.

As you'll see in the subsequent sections, it is not necessary for the sanitisation or destruction process to be completed directly by the company's IT staff. This further simplifies compliance with data protection obligations, as you can delegate the task to third-parties.

To fulfil the so-called quantum leap, it is vital to initially begin to think about security as a process and not as a product. Safety is first and foremost a cultural approach: you need a greater awareness of the problems related to the incorrect handling of data, and use appropriate IT tools to achieve defined security objectives. More specifically, because secure sanitisation and destruction have had to become a part of corporate culture and become more effective, it should not be left to the goodwill of individual users or even to the initiative of IT departments.

Cybersecurity-related spending is on track to surpass $133 billion in 2022, and the market has grown more than 30x in 13 years.

Data recovery and data protection

GDPR

The guide to the General Data Protection Regulation (GDPR) was formally adopted in 2016 and came into effect two years later in European Union member states. It is designed to tackle the challenges of personal data security and privacy in the age of the global, data-driven marketplace. Its basic principle is to protect subjects' data from loss or breach and gives a greater emphasis on transparency, giving data subjects a better understanding of how their information is stored, processed and deleted.

Under the GDPR, any individual or business handling or "processing" personal data must put in place appropriate technical and measures to implement the data protection principles. "Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data."

"Any organisation or business determining the purposes and means of processing personal data must design information systems with privacy in mind. No personal data may be processed unless it is done under one of six lawful bases specified by the regulation (consent, contract, public task, vital interest, legitimate interest or legal requirement). When the processing is based on consent, the data subject has the right to revoke it at any time." The punishment for breaking GDPR guidelines is severe – either fines of up to £20 million of 4% of global annual turnover (whichever is greater).

What is required to stay compliant?

Under Article 17 of the GDPR, individuals have the right to have their personal data permanently erased – known as 'The Right to be Forgotten.' "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay."

The GDPR does not specify what deletion means within the ambit of 'appropriate technical measures', but the Information Commissioner has issued guidance to say that personal data must be unrecoverable when disposing of hard drives and other data storage media. The Information Commissioner's Office (ICO) states that organisations must "ensure they delete personal data before recycling devices, so that data is not accessible to others after the device has left your ownership." Archiving data is therefore not considered as deletion. The suitable approach to data deletion will depend on how the device is being disposed of.

Resale

Any storage media that is resold must have been completely wiped. This means that all data must be sanitised to prevent any recovery. Ontrack has a range of erasure software solutions that offer 100% secure data erasure while leaving the device fully functional.

Recycling/Disposal

If the device is being recycled or otherwise disposed of, there is a broader choice of sanitisation options. Software deletion can be used, although it is relatively slow and cumbersome – particularly if there is a lot of hardware to be processed.

For devices that store data magnetically, the alternative is to use a tool like a degausser or a shredder both of which physically destroys each disk or piece of media by altering the magnetic fields that govern data storage in each disk platter, rendering the device completely unusable. The degaussing process takes approximately four seconds per unit, and the results are irreversible. It has the added benefit that it is also more cost-efficient than other physical destruction options as it can not only quickly process a much larger number of devices.

For devices that store data electronically, shredding is the best option for physical destruction. There can be specific requirements as to the size of the shredded bits.

ICO registration

Any data controller operating in the European Union is expected to register with the Information Commissioner's Office (ICO). Registration costs £35 per year for smaller companies and a £500 fee for businesses with a turnover of over £25.9 million. Registering is a legal requirement. You are also expected to report breaches of the GDPR direct to the ICO within 72 hours of becoming aware of the breach.

Technical measures for secure sanitisation

Under the GDPR, any organisation that processes personal data is required to handle it in accordance with the data protection principles. A data controller may use another organisation to process personal data on its behalf – a data processor, but the data controller remains responsible for ensuring its processing complies with the GDPR - whether it processes in-house or engages a data processor. In other words, companies don't need to take on the physical, secure sanitisation or destruction procedures themselves. Where there is a lack of appropriate skills, resources, and /or time allocation, you have the option to outsource this activity to competent suppliers, available in your area—but bear in mind the responsibility for the effectiveness of the process remains with you.

The technical measures for the secure deletion of data applicable to electronic devices are identified according to the following table:

If the device is intended for re-use and recycling, the actual data deletion can be completed with:	**Erasure software**
If the device is intended for disposal, you can also achieve secure deletion of optical storage or magneto-optical with the following procedures:	o Degaussing/shredding magnetic devices o Punching or mechanical deformation o Physical destruction or disintegration o High intensity demagnetisation

Erasure software

As the term suggests, the software will overwrite the existing data on the media by writing a new pattern of binary digits (ones and zeros) over it.

It is essential to consider that different media types (such as HDDs, SSDs and flash) will require different overwriting techniques to ensure the secure deletion of the data. The number of passes each type requires affects the time it takes for the erasure to complete, which can be a few hours or a few days, depending on the type of media and write speed.

Degaussing

A unique technique of permanent deletion of data applicable to memory devices based on a magnetic media (hard disk, floppy disk, magnetic tapes on open reels or cassette). It is able to ensure the rapid sanitisation of information from media where it is not possible to apply overwriting erasure software due to hardware failure.

How does degaussing work?

The physical principle underlying the degaussing relies on the polarisation of the Weiss domains.

The data is stored on magnetic media, such as hard disks and tapes, whereby a magnetic field is applied to very small areas called magnetic domains, specifically Weiss domains. This process is based on the theory developed by French physicist Pierre Weiss. The magnetic field whilst in the writing phase of the information impresses a verse that orients the magnetisation of a certain number of Weiss domains. These verses of the magnetisation are associated with the bit values 0 and 1.

By subjecting magnetic media to degaussing, the magnetisation arrangement of the Weiss domains that were generated when writing the data to the unit are no longer organised but forced into one direction, erasing the data.

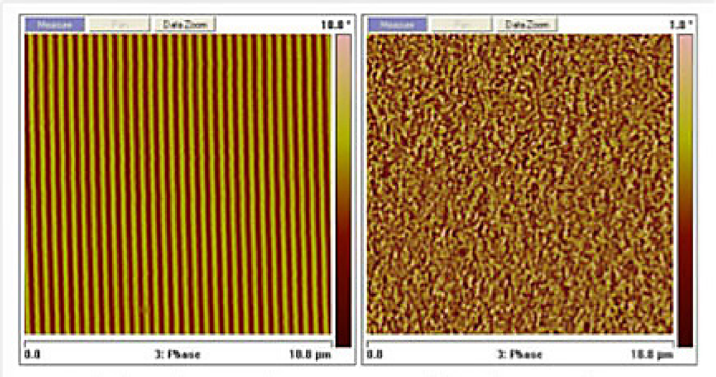
The demagnetisation process employs the use of an adequately powered hardware tool called a degausser. In contrast to overwriting software programmes, the time taken to complete an erasure through degaussing can be standardised, no matter what type of media or its data capacity. Another difference from overwriting erasure software is that a device subjected to demagnetisation is no longer reusable.

Punching or mechanical deformation

Punching refers to a procedure performed by pressing or hitting a punch on the surface of the device. This mechanically deforms the storage media making the data inaccessible.

Physical shredding or disintegration

This process is used to reduce storage media into fragments through the use of specific apparatuses equipped with suitable cutting blades e.g. a shredder.



Before degaussing

After degaussing

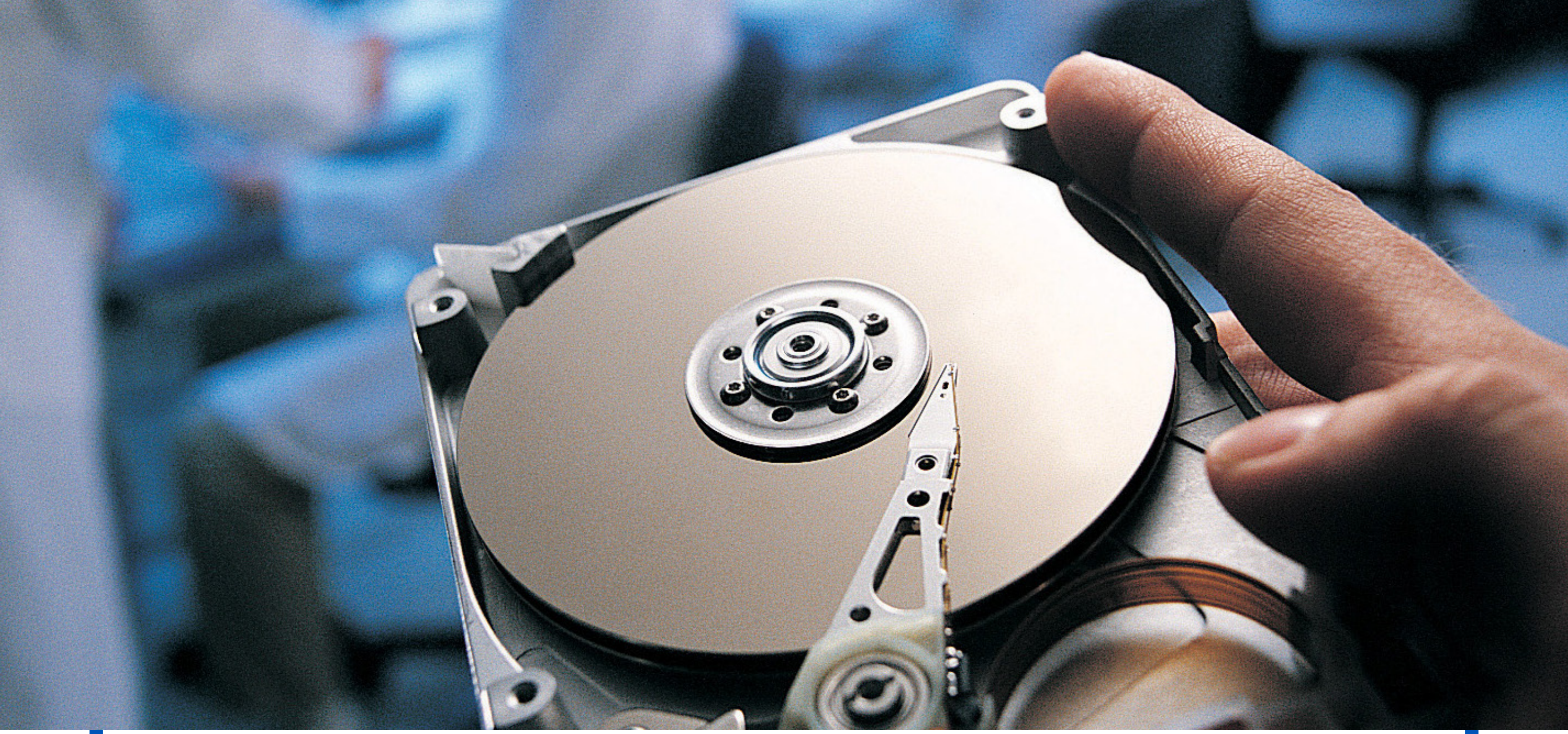
Image credit: Centre for Magnetic Recording Research (CMRR)

Devices subject to sanitisation

Devices subject to data sanitisation requirements include computers, desktops, laptops and servers as well as external storage media. It may also include items like network switches, routers cameras and other IoT devices. Any type of storage media containing personal data should be subject to safe sanitisation procedures and should include any device that contains information you want to keep private and confidential. Hard drives, SSDs, flash media of various types and formats, USB drives and magnetic tapes represent only a small sample of media to consider. A relatively new category of storage but an especially critical one is mobile devices.

Smartphones and tablets now offer considerable storage space and are considered standard equipment for most employees. According to data obtained by Statcounter, mobile devices are now more popular than desktops globally. It is therefore imperative when business mobile devices are withdrawn, to include them in the secure sanitisation process. It is important to note that smartphones and tablets contain the same information that you can find on devices such as desktop and laptop computers (e.g. email and documents) and even more data if we consider SMSs, phonebook and call logs.

According to data obtained by Statcounter, mobile devices are now more popular than desktops globally.



Professional tools to perform secure data sanitisation

The choice of software or hardware tools each company uses to perform a secure sanitisation process needs to be considered in detail. Not all tools on the market are effective and have suitable features to ensure business compliance with the current privacy legislation. It is also best to avoid do-it-yourself solutions as they are very risky in terms of effectiveness, and completely inadequate in providing a company with a professional and verifiable deletion certification or audit trail.

Ontrack solutions meet every requirement in the field of secure sanitisation and include:

- Software overwriting
- Hardware degaussing & drive shredding
- Services performed by specialised technicians

Software

Ontrack's data erasure software provides 100% sanitisation of targeted files, hard drives, SSDs, flash media, and mobile devices. With the option to choose from over 27 international erasure standards (incl. NIST 800-88 Purge), Ontrack's data erasure software programmes ensure that your sensitive data is permanently erased. The software validates the erasure process and generates comprehensive, tamper-proof reports, and certificates of erasure to comply with legal auditing requirements.

All of our data erasure products feature:

- An easy-to-use interface
- Fast and simultaneous erasure of multiple drives or media
- Are globally certified to meet international standards

Tamper-proof reports that support audit trails and data security & privacy regulations such as SOX, GLBA, HIPAA, ISO 27001, EU-GDPR, PCI-DSS, and many more.

GDPR EU General Data Protection Regulation

PCI Data Security Standard V 3.2

HIPAA COMPLIANT

Information Security Management ISO 27001 Certified

Ontrack’s data sanitisation solutions

Drive eraser

Ontrack drive eraser provides 100% data sanitisation of hard drives and solid-state drives, installed on PCs, laptops, servers, and enterprise storage systems.

Flash eraser

Our flash eraser software permanently erases data from removable media such as USB flash drives, SD cards, Microdrives, CompactFlash cards, and other storage devices.

Mobile eraser

Combines powerful diagnostic tests with secure mobile device erasure to increase efficiency, improve security, and guarantee compliance. Retailers, and Asset Disposition companies can rapidly process devices, certify data sanitisation, improve customer satisfaction, and increase overall profits.

File eraser

Selectively and securely erase sensitive files and folders from desktop computers, laptops, and servers to reduce the risk of a data breach, and achieve compliance with data security, and compliance regulations.

Hosted erase

Web-based data erasure solution that enables the simple execution and management of all your data sanitisation processes.

LUN eraser

Securely erase virtual machines, individual drives, and LUNs with ease, saving you time and money over physical destruction methods.

Hardware degaussing

Ontrack Eraser Degausser is a professional hardware device for data sanitisation through a demagnetisation (degaussing) process. It is one of the most powerful degaussers in the market, able to generate peak magnetic field strengths of up to 18,000 gausses (1.8 tesla), with 10,000 gausses (1 tesla) hitting the core of the device. A magnetic field of such power not only offers the guarantee of successful elimination of data from newer hard disks but also to safeguard the investment of the future with the use of disks that have a high recording density and coercivity factor.

Not all degaussers are able to delete data from hard drives and tapes permanently. You must bear in mind that a magnet opposes some resistance to demagnetisation - magnetic coercivity. Coercivity is the intensity of the reversed magnetic field that must be applied to a material to cancel its magnetisation. For a degausser to be effective, it is necessary that it is able to generate a magnetic field of at least equal to 1.5 times the coercivity of the support that needs to be deleted. What follows is that the higher the power of the degausser, the greater its effectiveness and the possibility to use it on future technology hard disks and other magnetic media. The degaussing procedure lasts only a few seconds; place the device in the compartment and push a button to initiate the demagnetisation. The media will not be reusable after this procedure.

Ontrack Eraser Degausser is effective and safe to use around people as well as other equipment and objects. The low-frequency magnetic field is concentrated in one area, where the action is well below the limits currently recommended by the ICNIRP—International Commission on Non-Ionising Radiation Protection—to the overall exposure of the general public.

Drive shredders

Ontrack can provide media shredders from several tested manufacturers to ensure your business disposes of its end of life hard drives, SSDs, smartphones, flash drives, tablets and more. Our drive shredders destroy based on the security Standard DIN 66399 reliable hard drives, solid-state devices and other data carriers/devices to provide complete eradication of all data.

Intimus HDD Granulator

Beyond secure degaussing, hard drive, and SSD shredders provide the best way to destroy storage devices and guarantee that data is irretrievable. Unique, hybrid technology that combines the benefits of shredding and disintegration.

Intimus FlashEx

The safest destroyer of your sensitive smartphones, mini-tablets and SSDs. The Intimus FlashEx is an ideal solution to your data erasure challenges. With a specially designed solid cutting head and unique cylinders, the FlashEx pulls material into the unit, crushing media into 4x15mm particles.

Intimus SSD Granulator

SSD granulator is a new technology that fits the erase need of businesses with larger volumes of SSDs, smartphones or other flash media. This shredder is designed for easy transport on stabile wheels, optimal for the volume capacity built into this powerful shredder. It handles all types of flash media, cut size is 5, 8 mm, and the security level is E-6 with a 3 mm screen.

https://docuvaultdv.com/how-to-securely-destroy-a-hard-drive/

Ontrack’s data sanitisation services

For companies that prefer to rely on a skilled third-party provider to fulfil their legal obligations or need to confirm the deletion process has been successful, Ontrack offers two types of services:

Services for secure data sanitisation

Technical personnel can perform sanitisation operations with the Ontrack Eraser software, Degausser and Shredder tools directly at the customer premises (on-site) or on the devices submitted to the Ontrack laboratory (in-house). The process is subsequently attested through an appropriate report, confirming the successful execution of the erasure process on the devices, which are then processed for disposal.

Erasure reporting services for audits/verification (Erasure Verification Services)

Erasure Verification Services are necessary to guarantee sanitisation of data on media intended for reuse or disposal. Organisations that do not verify the expunging of data on their media leave themselves open to accidental exposure or theft of sensitive data.

Devices are analysed by our technicians in our laboratories using sophisticated data recovery tools to identify any traces of user data. In the case of success (no trace data found), Ontrack will release a report as per the customer’s request confirming that it has been checked and the data erasure process used was adequate. If instead, we find traces of data, it will be immediately communicated to the customer so that they can make the necessary adjustments to their deletion process.

Conclusion

The introduction of global data privacy laws has attempted to standardise and update the protection of personal data as to face the new challenges of the digital era. It is therefore critical that organisations put secure erasure processes in place for end-of-life media that is due to be decommissioned/recycled, but also for through-life data during the regular lifecycle of devices.

For businesses, the easiest way to implement this is to set a budget aside at the time of purchasing any new hardware, and then utilise the service when the device needs to be disposed of or reused. Businesses may also decide to outsource this service to qualified third parties.

Overlooking end-of-life data and the incorrect management of data procedures, including the disposal of computers and IT assets containing personal data can become a serious threat to the security of company information; it also opens the company up to a potential risk for penalties and breaches of privacy legislation, which can cause irreparable damage to the businesses image and reputation.

Consider the following questions, when identifying your organisation's sanitisation protocol:

1. Does your organisation have a process for recycling end of life devices? Who is responsible?

2. Do you use a third party for this process? If so, how are you verifying that data has been completely sanitised from all storage media types?

3. What would be the impact on your business if company data was leaked due to improper sanitisation methods?

   - **Financial**
   - **Reputation and trust**
   - **Regulations and legal compliance**

4. If a customer contacted your business and invoked their right to have their personal data sanitised, do you have a process in place for identifying and erasing this data?

Your data experts

Ontrack is the data recovery and data destruction business of KLDiscovery, a global provider of ediscovery, information governance and data recovery solutions.

Ontrack has an award-winning suite of technology-driven services and software to help enterprises, service providers and government entities as well as consumers manage, recover, search, destroy, and migrate data efficiently and cost-effectively.

Experience that matters

With over 30 years' experience, Ontrack has developed strong roots and has an exciting, innovative future. Our strength in building great technology and delivering the highest quality services is the foundation for bringing exceptional data recovery solutions to our clients.

Data management solutions

With cleanroom facilities worldwide and engineering expertise in every major global region, you can count on us for all your data recovery, restoration and destruction needs.

Pioneers and innovators

Combining our deep industry experience and technological heritage, Ontrack brings you proprietary and best-in-class tools and capabilities across the data recovery spectrum.

24/7/365 service

Data loss can occur at any time, so we pride ourselves on providing our data recovery services around the clock. No matter the time or scenario, you can trust us to help with your data.

For more information on how Ontrack could help your organisation with your data sanitisation needs, please contact:

Yves Eng
Business Development Switzerland

Tel: +41 (0)44 877 30 90
M: +41 (0)79 815 61 63

Yves.Eng@ontrack.com